WHAT IS CLAIMED IS:

1. A computer program stored on a computer readable medium or a propagated signal for leveraging a persistent connection to provide a client access to a secured service, the computer program comprising:

an input code segment that causes a computer to receive input from a client;

a persistent connection code segment that causes the computer to establish a persistent connection with the client in response to a first request received through the input code segment from the client; and

a broker code segment that causes the computer to broker a connection between the client and a secured service based on a second request received through the input code segment from the client by leveraging the persistent connection with the client.

2. The computer program of claim 1 wherein:

the persistent connection is established based on keystone authentication information provided by the client; and

the broker code segment comprises a transparent authentication code segment that causes the computer to leverage the keystone authentication to authenticate the client without provision by the client of authentication information duplicative or additional to the keystone authentication information used to establish the persistent connection.

3. The computer program of claim 1 wherein:

the persistent connection is established based on keystone authentication information provided by the client; and

the broker code segment comprises a transparent authentication code segment that causes the computer to leverage the keystone authentication to authenticate the client without provision by the client of authentication information duplicative of the keystone authentication information used to establish the persistent connection.

4. The computer program of claim 1 wherein:

the persistent connection is established based on keystone authentication information provided by the client; and

the broker code segment comprises a transparent authentication code segment that causes the computer to leverage the keystone authentication to authenticate the client without provision by the client of authentication information additional to the keystone authentication information used to establish the persistent connection.

5. The computer program of claim 1 wherein the broker code segment causes the computer to broker the connection between the client and the secured service before the client attempts to connect to the secured service directly.

6. The computer program of claim 1 wherein the persistent connection code segment comprises:

a receiving code segment that causes the computer to receive keystone authentication information from the client;

a keystone authentication code segment that causes the computer to authenticate the client based on the keystone authentication information and to provide a keystone authentication associated with the persistent connection; and

a connection code segment that causes the computer to establish the persistent connection with the client based on the keystone authentication.

7. The computer program of claim 6 wherein the broker code segment includes a leveraging code segment that causes the computer to receive the second request from the client for connection to the secured service after the persistent connection to the client is established.

8. The computer program of claim 7 wherein the leveraging code segment further comprises:

a leveraged authentication code segment that causes the computer to provide a leveraged authentication based on the keystone authentication associated with the persistent connection; and

a leveraged connection code segment that causes the computer to use the leveraged authentication to establish the connection with the secured service.

9. The computer program of claim 8 wherein the leveraged authentication code segment comprises a transparent authentication code segment that causes the computer to provide the leveraged authentication based on the keystone authentication without provision by the client of authentication information duplicative or additional to the keystone authentication information used to establish the persistent connection.

10. The computer program of claim 1 wherein:

the persistent connection code segment includes a first partition code segment that causes the computer to establish the persistent connection between the client and a persistent connection service in response to the first request from the client; and

the broker code segment includes a second partition code segment that causes the computer to use a broker service to broker the connection between the client and the secured service based on the second request from the client.

11. The computer program of claim 10 wherein the second partition code segment comprises a reception code segment that causes the computer to receive from the persistent connection service at a connection request address a communication based on the second request from the client.

12. The computer program of claim 1 wherein the broker code segment comprises:

a liaison code segment that causes the computer program to communicate as an intermediary with the client and the secured service based on the second request from the client so that the client may obtain authorization information that may be used to establish the connection to the secured service;

a determining code segment that causes the computer to determine the authorization information based on the second request from the client;

a communication code segment that causes the computer to communicate to the secured service an indication that the client desires to connect to the secured service, wherein the indication comprises the authorization information;

a receiving code segment that causes the computer to receive a response from the secured service indicating that the client may be allowed to establish the connection to the secured service by presenting the authorization information to the secured service; and

an authorization code segment that causes the computer to communicate the authorization information to enable the client to present the authorization information to the secured service to establish the connection with the secured service.

13. The computer program of claim 1 wherein the broker code segment further comprises:

a liaison code segment that causes the computer program to communicate as an intermediary with the client and the secured service based on the second request from the client so that the client may obtain authorization information that may be used to establish the connection to the secured service;

a communication code segment that causes the computer to communicate to the secured service an indication that the client desires to connect to the secured service;

a receiving code segment that causes the computer to receive a response from the secured service indicating that the secured service may accept a connection from the client, wherein the response includes the authorization information;

an authorization code segment that causes the computer to communicate the authorization information to enable the client to present the authorization information to the secured service to establish the connection with the secured service.

14. The computer program of claim 13 wherein the response received by the computer from the secured service includes authorization information determined by the secured service.

15. The computer program of claim 1 wherein:

the broker code segment includes a liaison code segment that causes the computer program to communicate as an intermediary with the client and the secured service based on the second request from the client so that the client may obtain authorization information that may be used to establish the connection to the secured service;

the authorization information comprises constraint information; and

the authorization information may be ineffective to establish a connection with the secured service if the connection constraints are not satisfied by the constraint information.

16. The computer program of claim 15 wherein the connection constraints include a constraint that limits a number of uses for the authorization information to a predetermined threshold number.

17. The computer program of claim 16 wherein the connection constraints include a one-time-use password.

18. The computer program of claim 15 wherein the connection constraints include a constraint that the authorization information be used within a predetermined time window.

19. The computer program of claim 15 wherein the connection constraints include a constraint that the authorization information be presented to the secured service by a client for whom the connection was brokered.

20. A method of leveraging a persistent connection to provide a client access to a secured service, the method comprising:

receiving a first request from a client;

establishing a persistent connection with the client in response to the first request from the client;

receiving a second request from the client; and

brokering a connection between the client and a secured service based on the second request from the client by leveraging the persistent connection with the client.

21. The method of claim 20 wherein:

establishing the persistent connection with the client includes authenticating the client based on keystone authentication information provided by the client; and

brokering the connection between the client and the secured service includes leveraging the keystone authentication information to authenticate the client without provision by the client of authentication information duplicative or additional to the keystone information used to establish the persistent connection.

22. The method of claim 20 wherein :

establishing the persistent connection with the client includes authenticating the client based on keystone authentication information provided by the client; and

brokering the connection between the client and the secured service includes leveraging the keystone authentication information to authenticate the client without provision by the client of authentication information duplicative of the keystone information used to establish the persistent connection.

23. The method of claim 20 wherein :

establishing the persistent connection with the client includes authenticating the client based on keystone authentication information provided by the client; and

brokering the connection between the client and the secured service includes leveraging the keystone authentication information to authenticate the client without provision by the client of authentication information additional to the keystone information used to establish the persistent connection.

24. The method of claim 20 wherein the connection between the client and the secured service is brokered before the client attempts to connect to the secured service directly.

25. The method of claim 20 wherein establishing the persistent connection comprises:

receiving keystone authentication information from the client;

authenticating the client based on the keystone authentication information to provide a keystone authentication associated with the persistent connection; and

establishing the persistent connection with the client based on the keystone authentication.

26. The method of claim 25 wherein leveraging the persistent connection includes receiving the second request from the client for connection to the secured service after the persistent connection to the client is established.

27. The method of claim 26 wherein leveraging the persistent connection with the client includes:

providing a leveraged authentication based on the keystone authentication associated with the persistent connection; and

using the leveraged authentication to establish the connection with the secured service.

28. The method of claim 27 wherein the keystone authentication is used to provide the leveraged authentication without provision by the client of authentication information duplicative or additional to the keystone authentication information used to establish the persistent connection.

29. The method of claim 20 wherein;

the persistent connection is established between the client and a persistent connection service; and

the connection between the client and the secured service is brokered by a broker service.

30. The method of claim 29 wherein brokering the connection between the client and the secured service includes receiving from the persistent connection service at a connection request address a communication based on the second request from the client and wherein the connection request address varies systematically with time.

31. The method of claim 20 wherein brokering comprises:

receiving the second request from the client to connect to the secured service;

determining authorization information based on the second request from the client;

communicating to the secured service an indication that the client desires to connect to the secured service, wherein the indication comprises the authorization information;

receiving a response from the secured service indicating that the client may be allowed to establish the connection to the secured service by presenting the authorization information to the secured service; and

communicating the authorization information to enable the client to present the authorization information to the secured service to establish the connection with the secured service.

32. The method of claim 20 wherein brokering comprises:

receiving the second request from the client to connect to the secured service;

communicating to the secured service an indication that the client desires to connect to the secured service;

receiving a response from the secured service indicating that the secured service may accept a connection from the client, wherein the response includes authorization information; and

communicating the authorization information to enable the client to present the authorization information to the secured service to establish the connection with the secured service.

33. The method of claim 32 wherein the authorization information is determined by the secured service.

34. The method of claim 20 wherein:

brokering comprises communicating as an intermediary with the client and the secured service based on the second request from the client so that the client may obtain authorization information that may be used to establish the connection to the secured service;

the authorization information comprises constraint information; and

the authorization information may be ineffective to establish a connection with the secured service if the connection constraints are not satisfied by the constraint information.

35. The method of claim 34 wherein the connection constraints include a constraint that limits a number of uses for the authorization information to a predetermined threshold number.

36. The method of claim 34 wherein the connection constraints include a constraint that the number of times that the authorization information has been used not exceed a predetermined number of times.

37. The method of claim 34 wherein the connection constraints include a one-time-use password.

38. The method of claim 34 wherein the connection constraints include a constraint that the authorization information be used within a predetermined time window.

39. The method of claim 34 wherein the connection constraints include a constraint that the authorization information be presented to the secured service by a client for whom the connection was brokered.

40. A system for leveraging a persistent connection to provide a client access to a secured service, the system comprising:

input means for receiving input from a client;

persistent connection means for establishing a persistent connection with a client in response to a first request received through the input means from the client;

broker means for brokering a connection between the client and a secured service based on a second request received through the input means from the client by leveraging the persistent connection with the client.

41. The system of claim 40 wherein:

the persistent connection is established based on keystone authentication information provided by the client; and

the broker means comprises transparent authentication means for leveraging the keystone authentication to authenticate the client without provision by the client of authentication information duplicative or additional to the keystone authentication information used to establish the persistent connection.

42. The system of claim 40 wherein:

the persistent connection is established based on keystone authentication information provided by the client; and

the broker means comprises transparent authentication means for leveraging the keystone authentication to authenticate the client without provision by the client of authentication information duplicative of the keystone authentication information used to establish the persistent connection.

43. The system of claim 40 wherein:

the persistent connection is established based on keystone authentication information provided by the client; and

the broker means comprises transparent authentication means for leveraging the keystone authentication to authenticate the client without provision by the client of authentication information additional to the keystone authentication information used to establish the persistent connection.

44. The system of claim 40 wherein the broker means brokers the connection between the client and the secured service before the client attempts to connect to the secured service directly.

45. The system of claim 40 wherein the persistent connection means comprises:

receiving means for receiving keystone authentication information from the client;

keystone authentication means for authenticating the client based on the keystone authentication information to provide a keystone authentication associated with the persistent connection; and

connection means for establishing the persistent connection with the client based on the keystone authentication.

46. The system of claim 45 wherein the broker means includes leveraging means for receiving the second request from the client for connection to the secured service after the persistent connection to the client is established.

47. The system of claim 46 wherein the leveraging means further comprises:

leveraged authentication means for providing a leveraged authentication based on the keystone authentication associated with the persistent connection; and

leveraged connection means for causing the leveraged authentication to be used to establish the connection with the secured service.

48. The system of claim 47 wherein the leveraged authentication means comprises transparent authentication means for causing the leveraged authentication to be provided based on the keystone authentication without provision by the client of authentication information duplicative or additional to the keystone authentication information used to establish the persistent connection.

49. The system of claim 40 wherein:

the persistent connection means includes first partition means for establishing the persistent connection between the client and a persistent connection service in response to the first request from the client; and

the broker means includes second partition means for causing a broker service to be used to broker the connection between the client and the secured service based on the second request from the client.

50. The system of claim 49 wherein the second partition means comprises reception means for receiving from the persistent connection service at a connection request address a communication based on the second request from the client.

51. The system of claim 40 wherein the broker means further comprises:

liaison means for communicating as an intermediary with the client and the secured service based on the second request from the client so that the client may obtain authorization information that may be used to establish the connection to the secured service;

determining means for determining the authorization information based on the second request from the client;

communication means for communicating to the secured service an indication that the client desires to connect to the secured service, wherein the indication comprises the authorization information;

receiving means for receiving a response from the secured service indicating that the client may be allowed to establish the connection to the secured service by presenting the authorization information to the secured service; and

authorization means for communicating the authorization information to the client to enable the client to present the authorization information to the secured service to establish the connection with the secured service.

52. The system of claim 40 wherein the broker means further comprises:

liaison means for communicating as an intermediary with the client and the secured service based on the second request from the client so that the client may obtain authorization information that may be used to establish the connection to the secured service;

communication means for communicating to the secured service an indication that the client desires to connect to the secured service;

receiving means for receiving a response from the secured service indicating that the secured service may accept a connection from the client, wherein the response includes the authorization information;

authorization means for communicating the authorization information to the client to enable the client to present the authorization information to the secured service to establish the connection with the secured service.

53. The system of claim 52 wherein the response received by the receiving means includes authorization information determined by the secured service.

54. The system of claim 40 wherein:

the broker means includes liaison means for communicating as an intermediary with the client and the secured service based on the second request from the client so that the client may obtain authorization information that may be used to establish the connection to the secured service;

the authorization information comprises constraint information; and

the authorization information may be ineffective to establish a connection with the secured service if the connection constraints are not satisfied by the constraint information.